American Bar Association
www.supremecourtpreview.org

No. 07-513

IN THE

Supreme Court of the United States

BENNIE DEAN HERRING,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Writ of Certiorari to the United States Court of Appeals for the Eleventh Circuit

BRIEF OF *AMICI CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC), PRIVACY AND CIVIL RIGHTS ORGANIZATIONS, AND LEGAL SCHOLARS AND TECHNICAL EXPERTS IN SUPPORT OF PETITIONER

MARC ROTENBERG
Counsel of Record
MELISSA NGO
ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)
1718 Connecticut Ave., NW
Suite 200
Washington, DC 20009
(202) 483-1140

May 16, 2008

TABLE OF CONTENTS

TABLE OF CONTENTS ..... **i**

TABLE OF AUTHORITIES ..... **iii**

INTEREST OF THE *AMICI CURIAE* **1**

SUMMARY OF THE ARGUMENT **6**

ARGUMENT **7**

I. IN RECENT YEARS, THERE HAS BEEN A DRAMATIC EXPANSION OF LAW ENFORCEMENT DATABASES 8

A. The Rise of the Information Sharing Environment 8

B. State Fusion Centers Pose Unique Challenges to Criminal Justice Recordkeeping 9

II. NUMEROUS REPORTS DETAIL NUMEROUS ERRORS IN GOVERNMENT AND COMMERCIAL DATABASES 13

A. Problems with the National Crime Information Center ("NCIC") 13

B. Problems with Databases Associated with the Federal Government's Employment Eligibility Verification System 16

C. Commercial Databases on Which Law Enforcement Rely Are Also Inaccurate and Incomplete 18

D. Problems with Terrorist Watch Lists 20

1. Office of Foreign Assets Control's Specially Designated Nationals and Blocked Persons ("SDN") List 20

2. No-Fly and Selectee Lists 22

III. FEDERAL GOVERNMENT IS INCREASINGLY EXEMPTING DATABASES FROM ACCURACY AND PRIVACY REQUIREMENTS 28

A. Federal Privacy Act Accuracy Obligations 29

B. The National Crime Information Center Is Exempt From Key Requirements 32

C. The Automated Targeting System Is Exempt From Key Requirements 34

CONCLUSION 35

TABLE OF AUTHORITIES

CASES

Arizona v. Evans, 514 U.S. 1 (1995) 7, 35

Doe v. Chao, 540 U.S. 614 (2004) 31

STATUTES

28 U.S.C. § 534 (2002) 33

H.B. 1007, 2008 Gen. Assem., Spec. Sess. (Va. 2008) 13

Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (2004) 8, 9

Privacy Act of 1974. 5 U.S.C. § 552a ... 28, 31, 32, 33

OTHER AUTHORITIES

ARTHUR MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS (1971) 29

Audrey Hudson, *Air marshals' names tagged on 'no-fly' list*, Wash. Times, Apr. 29, 2008..... 27

Beverley Lumpkin, *Aviation Security Chief Says No-Fly List is Being Reduced by Half*, Associated Press, Jan. 18, 2007 28

Bob Sullivan, *ChoicePoint files found riddled with errors*, MSNBC, Mar. 8, 2005..... 19

Bob Sullivan, *Red Tape Chronicles: Bob the Writer, Bob the Molester*, MSNBC, May 3, 2006..... 20

Bureau of Justice Statistics, *Improving Access to and Integrity of Criminal History Records*, NCJ 200581 (July 2005)..... 14, 15

Bureau of Justice Statistics, *Improving Criminal History Records for Background Checks* (May 2003) 16

Bureau of Justice Statistics, *Report of the National Task Force on Privacy, Technology and Criminal Justice Information*, NCL 187669 (Aug. 2001) . 14

Bureau of Justice Statistics, *Use and Management of Criminal History Record Information: A Comprehensive Repor*t, 2001 Update, NCJ 187670 (Dec. 2001)..... 14, 15

Charles E. Allen, Chief Intelligence Officer, Dep't of Homeland Sec*., Hearing on the Assessment of Information Sharing Centers Before the Subcomm. on Intelligence, Info. Sharing, & Terrorism, H. Comm. on Homeland Sec.,* 109th Cong. (Sept. 7, 2006)..... 10

Comm'n of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (2006)..... 25, 26

Comm'n of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Factual Background, Vol. 1* (2006) 24

Comm'n of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Factual Background, Vol. 2* (2006). 25

Dep't of Health, Educ. & Welfare, Secretary's Advisory Comm. on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens* (MIT 1973) 30

Dep't of Homeland Sec., *Notice of Privacy Act System of Records: U.S. Customs and Border Protection, Automated Targeting System*, 72 Fed. Reg. 43,650 (Aug. 6, 2007)..... 34

Dep't of Justice, Bureau of Justice Statistics, National Criminal History Improvement Program (NCHIP)..... 15

Dep't of Justice, *Follow-Up Audit of the Terrorist Screening Center, Audit Report 07-41* (Redacted for Public Release) (Sept. 2007) 22, 23, 34

Ellen Nakashima, *A Good Name Dragged Down*, Wash. Post, Mar. 19, 2008..... 21

EPIC, "Joint Letter and Online Petition: Require Accuracy for Nation's Largest Criminal Justice Database (NCIC)" (Apr. 2003) 1

Exec. Order. No. 13,388, 3 C.F.R. 13,388 (2006). ... 9

Follow-Up Report on INS Efforts to Improve the Control of Nonimmigrant Overstays, Rept. No. I-2002-006 (Apr. 2002)..... 17

Global Justice Info. Sharing Initiative, Dep't of Justice, *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era -- Guidelines for Establishing and Operating Fusion Centers at the Local, State, and Federal Levels -- Law Enforcement Intelligence,*

Public Safety and the Private Sector (Aug. 2006) 10, 11, 12

Gov't Accountability Office, *Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information during Secure Flight Program Testing in Initial Privacy Notices, but Has Recently Taken Steps to More Fully Inform the Public*, GAO-05-864R (July 22, 2005)..... 27

Gov't Accountability Office, *Immigration Enforcement: Weaknesses Hinder Employment Verification and Worksite Enforcement Efforts,* GAO-05-813 25 (Aug. 2005) 17

Gov't Accountability Office, *Terrorist Watch List Screening: Efforts to Help Reduce Adverse Effects on the Public,* GAO-06-1031 (Sept. 2006)..... 27

Immigration and Naturalization Service's Ability to Provide Timely and Accurate Alien Information to the Social Security Administration, Rept. No. I-2003-001 (Nov. 2002) 17

Jane Black, *Data Collectors Need Surveillance, Too,* Business Week, Jan. 24, 2002..... 19

Kim Zetter, *Bad Data Fouls Background Checks*, Wired News, Mar. 11, 2005..... 19

Lawyers' Comm. for Civil Rights of the San Francisco Bay, *Complaints Released by Treasury Department*, Mar. 17, 2008..... 21, 22

Leslie Miller, *House Transportation Panel Chairman Latest to be Stuck on No-Fly List*, Associated Press, Sept. 29, 2004..... 28

Letter from Alberto Gonzales, U.S. Atty. Gen., and Michael Chertoff, Sec'y, Dep't of Homeland Sec., to Stockwell Day, Canadian Minister of Public Safety (Jan. 16, 2007) 26

Letter from Virginia R. Canter, Associate Dir., Resource Mgmt., Office of Foreign Assets Control, to Thomas R. Burke, Davis Wright Tremaine LLP (Mar. 17, 2008) 21

Michael Chertoff, Sec'y, Dep't of Homeland Sec., *Remarks at the International Association of Chiefs of Police Annual Conference* (Oct. 16, 2006) 10

Office of Foreign Assets Control, Frequently Asked Questions..... 20, 21

Office of Inspector Gen., Dep't of Justice, *Immigration and Naturalization Service Monitoring of Nonimmigrant Overstays, Rept. No. I-97-08* (Sept. 1997)..... 17

Office of Inspector Gen., Soc. Sec. Admin, *Congressional Response Report: Accuracy of the Social Security Administration's NUMIDENT File, A-08-06-26100* (Dec. 18, 2006) 17

Press Release, Federal Bureau of Investigation (July 15, 1999)..... 14

Privacy Office, Dep't of Homeland Sec., *Report Assessing the Impact of the Automatic Selectee and No Fly Lists on Privacy and Civil Liberties as Required Under Section 4012(b) of the Intelligence Reform and Terrorism Prevention Act of 2004* (Apr. 27, 2006)..... 23

Privacy Protection Study Comm'n, *Personal Privacy in an Information Society* (July 1977).. 32

Ryan Singel, *Nun Terrorized by Terror Watch*, Wired News, Sept. 26, 2005 24

S. Rep. No. 93-1183 (1974)..... 30, 31

SAMUEL ALITO, THE BOUNDARIES OF PRIVACY IN AMERICA (1972) ("Report of the Chairman") 36

Sara Kehaulani Goo, *Committee Chairman Runs Into Watch-List Problem*, Wash. Post, Sept. 30, 2004 28

Shaun Waterman, *Senator Gets a Taste of No-Fly List Problems*, United Press Int'l, Aug. 20, 2004 28

The Computer and the Invasion of Privacy: Hearings Before a Subcom. of the H. Comm on Gov't Operations, 89th Cong. (1966)..... 29

Thomas E. Bush III, Assistant Dir., Criminal Justice Info. Serv. Div., *Statement Before the S. Comm. on Homeland Sec. & Gov'tal Affairs*, 109th Cong. (June 29, 2005) 22

Todd Masse, Siobhan O'Neil & John Rollins, Cong. Research Serv., *Fusion Centers: Issues and Options for Congress, RL34070* (July 6, 2007)..... 9, 10

Transp. Sec. Admin., Dep't of Homeland Sec., *Complaint Log: Nov. 2003 to May 2004*..... 23

INTEREST OF THE *AMICI CURIAE*[1]

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., which was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values. EPIC has participated as *amici* in several cases before this Court, and other courts, concerning privacy issues and new technologies. EPIC has a particular interest in the accuracy of government databases as it has routinely urged federal agencies to comply with the Privacy Act accuracy requirements. *See, e.g.,* Online Petition to Mitchell E. Daniels, Jr., Director, Office of Management and Budget (Apr. 7, 2003).[2]

---

[1] Letters of consent to the filing of this brief have been lodged with the Clerk of the Court pursuant to Rule 37.3. Counsel of record for all parties received notice at least 10 days prior to the due date of the amicus curiae's intention to file this brief. In accordance with Rule 37.6 it is stated that no counsel for a party authored this brief in whole or in part, and no counsel or party made a monetary contribution intended to fund the preparation or submission of this brief. No person other than *amicus curiae*, its members, or its counsel made a monetary contribution to its preparation or submission. EPIC IPIOP clerk Sobia Virk assisted in the preparation of this brief.

[2] EPIC, "Joint Letter and Online Petition: Require Accuracy for Nation's Largest Criminal Justice Database (NCIC)" (Apr. 2003) ("We strongly oppose the Justice Department's recent decision to lift the Privacy Act requirement that the FBI ensure the accuracy and completeness of the over 39 million criminal records it maintains in its National Crime Information Center

Amici Technical Experts and Legal Scholars

Steven Aftergood, Project Director, Federation of American Scientists

Anita L. Allen, J.D., Ph.D., Henry R. Silverman Professor of Law and Professor of Philosophy, University of Pennsylvania Law School

Annie I. Antón, Professor of Computer Science, North Carolina State University

David Banisar, Deputy Director, Privacy International; Non-Resident Fellow, The Center for Internet and Society, Stanford Law School

Ann Bartow, Associate Professor of Law, University of South Carolina School of Law

Francesca Bignami, Professor of Law, Duke University School of Law

James Boyle, William Neal Reynolds Professor of Law, Duke University School of Law

Simon Davies, Visiting Senior Fellow, Department of Management, London School of Economics

David J. Farber, Distinguished Career Professor of Computer Science and Public Policy, Carnegie Mellon University

Phil Friedman, Friedman Law Offices, PLLC

Austin Hill, Brudder Technology Ventures

Deborah Hurley, Chair, EPIC Advisory Board

Jerry Kang, Professor of Law, UCLA School of Law

Chris Larsen, CEO, Prosper Marketplace, Inc.

Gary T. Marx, Professor Emeritus of Sociology, M.I.T.

Mary Minow, LibraryLaw.com

(NCIC) database."), *available at* http://epic.org/privacy/ncic/.

Pablo Molina, Chief Information Officer, Georgetown University Law Center

Dr. Peter Neumann, Principal Scientist, SRI International Computer Science Lab

Ray Ozzie, Chief Software Architect, Microsoft

Dr. Deborah Peel, Founder, Patient Privacy Rights

Anita Ramasastry, Associate Professor of Law, University of Washington School of Law

Ronald L. Rivest, Andrew and Erna Viterbi Professor of Electrical Engineering and Computer Science, MIT Department of Electrical Engineering and Computer Science

Pamela Samuelson, Richard M. Sherman Distinguished Professor of Law & Information, University of California, Berkeley

Dr. Bruce Schneier, Chief Technical Officer, BT Counterpane

Daniel J. Solove, Associate Professor of Law, George Washington University Law School

Frank Tuerkheimer, Professor of Law Emeritus, University of Wisconsin Law School

Edward G. Viltz, www.InternetCC.org

Amici Civil Liberties and Privacy Organizations

The Asian American Justice Center is a national non-profit, non-partisan organization whose mission is to advance the human and civil rights of Asian Americans. AAJC and its Affiliates have a long-standing interest in this case because the inaccuracy of government databases have a significant impact on implementation of the laws and policies as they are applied to the Asian American community, and this interest has resulted in AAJC's participation in a number of administrative rulemaking comments and *amicus* briefs before the courts.

The Asian American Legal Defense and Education Fund, founded in 1974, defends the civil rights of Asian Americans nationwide through litigation, legal advocacy and dissemination of public information.

The Center for Democracy & Technology is a non-profit, non-partisan public interest organization dedicated to developing and implementing public policies to protect and advance civil liberties and democratic values on the Internet and in the digital age.

The Electronic Frontier Foundation is a non-profit, member-supported civil liberties organization working to protect rights in the digital world.

The Gun Owners of America is a national grassroots lobby organization defending the Second Amendment in Congress and the Courts.

The Identity Project provides advice, assistance, publicity, and legal defense to those who find their rights infringed, or their legitimate activities curtailed, by demands for identification, and builds public awareness about the effects of ID requirements on fundamental rights.

The Liberty Coalition works to help organize, support, and coordinate transpartisan public policy activities related to civil liberties and basic rights. We work in conjunction with groups of partner organizations that are interested in preserving the Bill of Rights, personal autonomy and individual privacy.

The Multiracial Activist is a libertarian oriented activist journal focusing on civil liberties issues, multiracial individuals and interracial families.

The National Federation of Filipino American Associations is a nonprofit, nonpartisan civil rights organization dedicated to promoting the interests

and betterment of Filipinos and Filipino Americans in the United States and to ensure that Asian Pacific Americans enjoy equal opportunities in education, employment, and industry.

The National Immigration Law Center is a national legal advocacy organization whose mission is to protect and promote the rights and opportunities of low-income immigrants and their families.

OpenTheGovernment.org is a coalition of consumer and good government groups, journalists, environmentalists, library groups, labor and others united to make the federal government a more open place in order to make us safer, strengthen public trust in government, and support our democratic principles.

The Rutherford Institute is a non-profit conservative legal organization dedicated to the defense of civil, especially religious, liberties and human rights.

The Workmen's Circle/Arbeter Ring is a 107-year-old national Jewish organization dedicated to Jewish culture, community and social justice.

SUMMARY OF THE ARGUMENT

The technology of government databases has changed dramatically since 1995, when the Court upheld the use of evidence obtained from an erroneous arrest record that was the product of a clerical mistake. Today, the police have within their electronic reach access to an extraordinary range of databases including: the National Crime Information Center, systems associated with the federal government's employment eligibility verification system, terrorist watch lists and various commercial databases.

These government and commercial databases are filled with errors, according to the federal government's own reports. Yet the government has further compounded the problems with record inaccuracies with two decisions: first, the increased distribution of the data not just among government agencies but among federal, state, local, tribal and commercial entities; and second, the exemption of database systems from important privacy and accuracy requirements set out in federal laws. To allow law enforcement agencies to rely on inaccurate data will exacerbate further a problem that implicates both the fairness of the criminal justice system as well as the design and operation of government information systems.

Given the consequences that may flow from law enforcement officials acting upon errors in these systems, *amici* believe it is critical for the Court to ensure an accuracy obligation on law enforcement agents who rely on criminal justice information systems. In this context, to permit a good faith reliance on data that is inaccurate, incomplete, or out of date will actually exacerbate the problem

and increase the likelihood of unfair treatment in the criminal justice system.

ARGUMENT

Justice O'Connor's concurrence in *Arizona v Evans* stated clearly the danger of reliance on error-prone recordkeeping systems. *Arizona v. Evans*, 514 U.S. 1, 16-17 (1995):

> [w]hile the police were innocent of the court employee's mistake, they may or may not have acted reasonably in their reliance *on the recordkeeping system itself*. Surely it would *not* be reasonable for the police to rely, say, on a recordkeeping system, their own or some other agency's, that has no mechanism to ensure its accuracy over time and that routinely leads to false arrests, even years after the probable cause for any such arrest has ceased to exist (if it ever existed).

Id. at 17 (emphasis in original).

As technology evolves, law enforcement officials are increasingly using a vast, cross-referenced system of public and private databases, which contains numerous errors. In these interlinked databases, one error can spread like a disease, infecting every system it touches and condemning the individual to whom this error refers to suffer substantial delay, harassment, and improper arrest. Accuracy requirements ensure not only fairness in the criminal justice system, but also the effective and efficient use of law enforcement resources. In the absence of such obligations, more individuals will be subject to improper arrest as the data on which the criminal justice system depends

becomes increasingly outdated, incomplete, and inaccurate.

I. In Recent Years, There Has Been a Dramatic Expansion of Law Enforcement Databases

In recent years, there has been an increase in information sharing not just among government agencies but among federal, state, local, tribal and commercial entities. The broad data-gathering and sharing through the Information Sharing Environment and the state and local fusion centers has changed the policies and practices of modern-day policing. Today's law enforcement interactions do not merely involve one sheriff's clerk calling a clerk in another county. Instead, law enforcement personnel access a massive interconnected web of databases that contains myriad inaccurate data, which can provide the basis for wrongful arrests.

A. The Rise of the Information Sharing Environment

In December 2004, Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004, which directed the president to "create an information sharing environment for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties." Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (2004). Notably, the Act defined "information sharing environment" as "an approach that facilitates the sharing of terrorism information, which approach may include any methods determined necessary and appropriate for carrying out this section." *Id*.

In October 2005, President George W. Bush issued Executive Order 13,388, "Further Strengthening the Sharing of Terrorism Information To Protect Americans," which created the Information Sharing Environment among these many entities. Exec. Order. No. 13,388, 3 C.F.R. 13,388 (2006). The Information Sharing Environment Program (managed by former Ambassador Thomas E. McNamara) was placed under the Office of the Director of National Intelligence (J. Mike McConnell).

B. State Fusion Centers Pose Unique Challenges to Criminal Justice Recordkeeping

An outgrowth of the expansion of criminal justice data sharing has been "fusion centers," which have received $380 million in federal grants and millions more from state governments. Todd Masse, Siobhan O'Neil & John Rollins, Cong. Research Serv., *Fusion Centers: Issues and Options for Congress, RL34070* 20, 93 (July 6, 2007) [hereinafter "CRS Fusion Centers Report"]. There are 43 current and planned fusion centers in the U.S., and some states have more than one. *Id*. at 2.

State fusion centers began as "the outgrowth or expansion of an existing intelligence and/or analytical unit or division within the state's law enforcement agency." *Id*. at 19. However, the presence of Department of Homeland Security ("DHS") officials has grown. The agency has "embedded" federal officials at many local and state fusion centers, and has said it seeks to deploy federal staff to all of them. Charles E. Allen, Chief Intelligence Officer, Dep't of Homeland Sec., *Hearing on the Assessment of Information Sharing Centers Before the Subcomm. on Intelligence, Info.*

Sharing, & Terrorism, H. Comm. on Homeland Sec., 109th Cong. (Sept. 7, 2006) [hereinafter "DHS Testimony on Fusion Centers"].

In a July 2007 report, the Congressional Research Service ("CRS") interviewed "the majority of state fusion center leaders and operational directors . . . [and] stakeholders within the federal government" to learn more about fusion centers. CRS Fusion Centers Report at 93. CRS found that, though local and state fusion centers were originally designed to be local- or state-wide in jurisdiction and purely oriented toward counterterrorism, "they have increasingly gravitated toward an all-crimes and even broader all-hazards approach." *Id*. at i. A part of this broadening of fusion center missions is the DHS's goal of creating a "national network" of fusion centers, said Michael Chertoff, Secretary of DHS. Michael Chertoff, Sec'y, Dep't of Homeland Sec., *Remarks at the International Association of Chiefs of Police Annual Conference* (Oct. 16, 2006).

The federal Fusion Center Guidelines recommend that fusion centers "allow for future connectivity to other local, state, tribal, and federal systems." Global Justice Info. Sharing Initiative, Dep't of Justice, *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era -- Guidelines for Establishing and Operating Fusion Centers at the Local, State, and Federal Levels -- Law Enforcement Intelligence, Public Safety and the Private Sector* 2 (Aug. 2006) [hereinafter "DOJ Fusion Center Guidelines"]. Also, the federal Guidelines recommend that, "nontraditional collectors of intelligence, such as public safety

entities and private sector organizations" could be "'fused' with law enforcement data."[3] *Id.* at 3.

The federal Fusion Center Guidelines recommend that state fusion centers collect information on:

> Agriculture, Food, Water and the Environment, Banking and Finance, Chemical Industry and Hazardous Materials, Criminal Justice, Retail, Real Estate, Education, Emergency Services (Non-Law Enforcement), Energy, Government, Health and Public Health Services, Hospitality and Lodging, Information & Telecommunications, Military Facilities and Defense Industrial Base, Postal and Shipping, Private Security, Public Works, Social Services, [and] Transportation.

Id. at C-1.

State fusion centers can find this data by accessing a variety of government and commercial systems, such as:

- Driver's license,
- Motor vehicle registration,
- Location information (411, addresses, and phone numbers),
- Law enforcement databases,
- National Crime Information Center (NCIC),

---

[3] We note, but will not discuss the fact that use of private sector data in a national network of fusion centers raises the possibility that such data could be misused, allowing the government to circumvent warrant requirements and state or federal privacy laws or regulations. This possibility is not directly relevant to the issue at hand, but is still important.

- Nlets -- The International Justice and Public Safety Information Sharing Network, and the Terrorist Screening Center (TSC),
- Criminal justice agencies,
- Public and private sources (Security Industry databases, Identity Theft databases, Gaming Industry databases),
- Regional Information Sharing Systems (RISS)/Law Enforcement Online (LEO), U.S. Department of Homeland Security's (DHS) Homeland Security Information Network (HSIN), including the United States Private-Public Partnership (USP3) – formerly HSIN-CI. (Note: RISS, LEO, and DHS's HSIN are currently collaborating on a network capability.),
- Organizational and association resources (InfraGard, The Infrastructure Security Partnership),
- Corrections,
- Sex offender registries,
- Violent Criminal Apprehension Program (VICAP),
- Health- and Public Health-Related Databases (Public Health Information Network, Health Alert Network). *Id.* at 33-34.

This increased data dissemination is problematic for many reasons, including the fact that fusion centers use erroneous information culled from government and commercial databases. Moreover, law enforcement personnel rely on these new integrated state databases even as states are suspending the privacy obligations and open government requirements that would otherwise require public accountability in the management of these systems. In the state of Virginia, for example, legislation was recently enacted that would

suspend the application of the Virginia Freedom of Information Act and the Virginia Collection and Dissemination Practices Act to the Virginia Fusion Center. H.B. 1007, 2008 Gen. Assem., Spec. Sess. (Va. 2008). In other words, at the same time that the states are incorporating new technology that makes possible the expansion of data exchange in the criminal justice system, they are seeking to remove the legal obligations that would help ensure accuracy, reliability and accountability. It is this problem that is squarely before the Court in this case.

II. Numerous Reports Detail Numerous Errors in Government and Commercial Databases

Increasingly, law enforcement officials and other government employees are relying on government and commercial databases full of mistakes that are well-documented but rarely corrected. Government systems include the National Crime Information Center database and databases associated with the federal government's employment eligibility verification system. Commercial databases include information from databrokers such as Choicepoint. As these errors are distributed to various law enforcement and other groups through the Information Sharing Environment and fusion centers, enormous difficulties are created for innocent individuals.

A. Problems with the National Crime Information Center ("NCIC")

The National Crime Information Center ("NCIC") is a system that makes criminal history information widely available to police officers and law enforcement officials across the United States.

See generally Bureau of Justice Statistics, *Report of the National Task Force on Privacy, Technology and Criminal Justice Information*, NCL 187669, at 47 (Aug. 2001); *see also* Press Release, Federal Bureau of Investigation (July 15, 1999).

The problem of record accuracy has plagued the system for years. According to the Bureau of Justice Statistics, "[i]n the view of most experts, inadequacies in the accuracy and completeness of criminal history records is *the single most serious deficiency* affecting the Nation's criminal history record information systems." Bureau of Justice Statistics, *Use and Management of Criminal History Record Information: A Comprehensive Repor*t, 2001 Update, NCJ 187670 at 38 (Dec. 2001) (emphasis added).

In a 2005 report (the most recent report), the Department of Justice Bureau of Justice Statistics ("BJS") detailed ongoing concerns about errors in NCIC databases. Bureau of Justice Statistics, *Improving Access to and Integrity of Criminal History Records*, NCJ 200581 (July 2005). The BJS points to problems with State criminal history records, which are fed into the NCIC. "Recent BJS surveys have suggested that criminal history repositories are encountering several problems including significant backlogs, older records that have no dispositions, and infrequent audits to ensure accuracy of records." *Id*. at 11. Also, "Repositories in States that could estimate the size of their backlogs in 2001 reported that 2.5 million records of arrest, disposition, and custody information were unprocessed or only partially processed." *Id*. at 13.

Though the errors are well-known, the BJS found that audits of these records are infrequent. "In 2001, 23 State criminal history repository

directors reported that their databases had not been audited for completeness in the prior 5 years. […] Over half of those States (13) reported that they had not planned or scheduled a data quality audit to occur within the next 3 years. Overall, 24 States did not plan to perform a data quality audit within 3 years of the survey." *Id*.

The BJS said in 2001 that, if incomplete or inaccurate records are used *"there is a substantial risk that the user will make an incorrect or misguided decision*." *Id* (emphasis added*)*. Because the criminal history information is available to both private and public entities, misguided decisions may lead to an unjustified arrest, a lost employment opportunity, or inability to purchase a firearm. *Id*. There have not been many "in-depth audits or reviews of the accuracy of the information maintained by State and Federal criminal history record repositories" conducted, according to the report, but "most of those that have been conducted have found unacceptable levels of inaccuracies." *Id*. at 39.

The Department of Justice has sought to address concerns about record accuracy through the National Criminal History Improvement Program ("NCHIP"). Dep't of Justice, Bureau of Justice Statistics, National Criminal History Improvement Program (NCHIP).[4] The goal of the program is to "insure that accurate records are available for use in law enforcement," and to provide "direct funding and technical assistance to the States to improve the quality, timeliness and immediate accessibility of criminal history and related records." *Id*. Between 1995 and 2002, more

---

[4] http://www.ojp.usdoj.gov/bjs/nchip.htm (last visited May 6, 2008).

than $390 million dollars were allocated under the NCHIP program. Bureau of Justice Statistics, *Improving Criminal History Records for Background Checks* (May 2003).[5]

Nonetheless, as the 2005 BJS report makes clear, record accuracy continues to plague the criminal justice system. And with the continued expansion of the NCIC and the growth of fusion centers, the problem will become more severe.

B. Problems with Databases Associated with the Federal Government's Employment Eligibility Verification System

The problem of record accuracy reaches across the federal government. Several reports highlight inaccuracies in the government database used for employment verification. The errors in the federal government's employment eligibility verification system ("EEVS") are so egregious and their effects so significant, that a federal judge cited to them in an opinion granting a temporary restraining order against the Department of Homeland Security.

The government reports documenting the errors in databases connected with EEVS date back more than 10 years. In a 1997 report and a 2002 follow-up review, the Inspector General of the Department of Justice found that data from the Immigration and Naturalization Service (the predecessor of U.S. Citizenship and Immigration Services) were unreliable and "seriously flawed in content and accuracy." Office of Inspector Gen., Dep't of Justice, *Immigration and Naturalization Service Monitoring of Nonimmigrant Overstays,*

---

[5] *Available at* http://www.ojp.gov/bjs/abstract/ichrbc.htm (last visited May 6, 2008).

Rept. No. I-97-08 (Sept. 1997); *Follow-Up Report on INS Efforts to Improve the Control of Nonimmigrant Overstays, Rept. No. I-2002-006* (Apr. 2002); and *Immigration and Naturalization Service's Ability to Provide Timely and Accurate Alien Information to the Social Security Administration, Rept. No. I-2003-001* (Nov. 2002).

In August 2005, the Government Accountability Office investigated and found myriad errors in information from DHS databases searched through its employment eligibility verification system. Gov't Accountability Office, *Immigration Enforcement: Weaknesses Hinder Employment Verification and Worksite Enforcement Efforts,* GAO-05-813 25 (Aug. 2005).

A December 2006 report by the Social Security Administration's Office of Inspector General found accuracy problems in databases of Citizenship and Immigration Services and Social Security Administration. Office of Inspector Gen., Soc. Sec. Admin, *Congressional Response Report: Accuracy of the Social Security Administration's NUMIDENT File, A-08-06-26100* (Dec. 18, 2006). The Inspector General estimated that about 17.8 million records in the Social Security Administration's Numerical Identification File ("NUMIDENT") have discrepancies with name, date of birth or death, or citizenship status. *Id*. at 6. About 13 million of these incorrect records belong to U.S. citizens, he said. *Id*. at Appendix C-2.

A federal judge pointed to the problems in NUMIDENT in an October 2007 opinion granting a temporary restraining order enjoining the Department of Homeland Security from implementing a new "no-match" employment eligibility verification proposal.

> As demonstrated by plaintiffs, the government's proposal to disseminate no-match letters affecting more than eight million workers will, under the mandated time line, result in the termination of employment to lawfully employed workers. This is so because, as the government recognizes, the no-match letters are based on SSA records that include numerous errors.

AFL-CIO v. Chertoff, No. C 07-04472 CRB 7 (N.D. Cal. 2007).

It is clear that the federal government's employment eligibility verification system is based on erroneous databases. As fusion centers continue to mix and mingle data from a multitude of government databases, such information is becoming more accessible to law enforcement officials in the criminal justice context. This strongly implicates the accuracy and reliability of the criminal justice system.

Multiple government assessments state that the watch lists remain filled with errors. The Justice Department Inspector General has said this indicates "a deficiency in the integrity of watchlist information." Justice Dept. Report on Watch Lists at xxii. These watch lists are used to screen "approximately 270 million individuals . . . each month." *Id*. at v. Such mistakes show it is paramount that government entities are held accountable for accuracy of their databases.

C. Commercial Databases on Which Law Enforcement Rely Are Also Inaccurate and Incomplete

There is extensive documentation of errors in commercial databases, as well. The government

has increasingly relied upon these databases in its law enforcement activities and, as explained earlier, the federal Fusion Center Guidelines urge the intermingling of commercial data with information culled from government systems. For example, databroker Choicepoint trumpets on its Web site the various federal, state, local and law enforcement "solutions" that the company offers.[6] These reports often include information that is erroneous, out of date, incomplete, unreliable, or just flat-out false.

A man bought his Choicepoint record and found that the file showed he had died in 1976. Jane Black, *Data Collectors Need Surveillance, Too,* Business Week, Jan. 24, 2002. Another man's report included numerous crimes that he never committed. "In Florida I'm a female prostitute (named Ronnie); in Texas I'm currently incarcerated for manslaughter," according to the man. Kim Zetter, *Bad Data Fouls Background Checks*, Wired News, Mar. 11, 2005. Also, "In New Mexico I'm a dealer of stolen goods. Oregon has me as a witness tamperer. And in Nevada -- this is my favorite -- I'm a registered sex offender." *Id*.

Another Choicepoint file contained significant errors. The record of one woman listed "possible Texas criminal history" even though she has been to Texas only twice and has not been charged with or committed crimes there. Bob Sullivan, *ChoicePoint files found riddled with errors*, MSNBC, Mar. 8, 2005. Her record also included "three automobiles she never owned and three companies listed that she never owned or worked for." *Id*.

---

[6] http://www.choicepoint.com/ (last visited May 6, 2008).

When a news reporter looked up his file on databroker Intellius.com, he found the record said he was charged with child molestation (he wasn't) and that he had a close male relative who was convicted of manslaughter (the reporter had never even heard of the man). Bob Sullivan, *Red Tape Chronicles: Bob the Writer, Bob the Molester*, MSNBC, May 3, 2006.

These are just a few of the many erroneous records that have been compiled by Choicepoint and other databrokers used by the federal government for law enforcement purposes.

D. Problems with Terrorist Watch Lists

The federal government manages at least three terrorist watch lists: the no-fly and selectee lists, which are managed by the Terrorist Screening Center, and the Specially Designated Nationals and Blocked Persons ("SDN") list, which is managed by the Treasury Department's Office of Foreign Assets Control ("OFAC"). All of these lists have been criticized for their errors, which can be compounded by the opacity of the process behind the lists.

1. Office of Foreign Assets Control's Specially Designated Nationals and Blocked Persons ("SDN") List

According to OFAC, the SDN list "includes over 6,000 names of companies and individuals who are connected with the sanctions targets and are located throughout the world." Office of Foreign Assets Control, Frequently Asked Questions.[7] "U.S. persons are prohibited from dealing with SDNs

[7] http://www.treas.gov/offices/enforcement/ofac/faq/answer.shtml (last visited May 6, 2008).

wherever they are located and all SDN assets are blocked." *Id*. This list has caused significant problems because an increasing number of individuals are mismatched to this list as private businesses, such as banks, car dealerships, employers and landlords, run applicants' names against the SDN list.

In March, the Treasury Department released documents under a Freedom of Information Act request from the Lawyers' Committee for Civil Rights of the San Francisco Bay area. Letter from Virginia R. Canter, Associate Dir., Resource Mgmt., Office of Foreign Assets Control, to Thomas R. Burke, Davis Wright Tremaine LLP (Mar. 17, 2008).[8] Included in the documents were complaints from individuals who had been denied mortgages or otherwise negatively affected because they were mistakenly matched to a name on the OFAC list and a "red flag" or some other alert was put on their credit reports. *Id*. *See also*, Ellen Nakashima, *A Good Name Dragged Down*, Wash. Post, Mar. 19, 2008.

A former Naval officer, a police officer and a 30-year employee of the Department of Defense were among the individuals who were mistakenly matched and who had difficulty getting the SDN label off their credit reports. Lawyers' Comm. for Civil Rights of the San Francisco Bay, *Complaints Released by Treasury Department*, Mar. 17, 2008.[9] These individuals contacted OFAC, the FBI, and their Congressional representatives in efforts to clear their names. The complaints reveal the

---

[8] http://www.lccr.com/3%2018%2008%20Treasury%20Dept%20Cover%20Letter.pdf (last visited May 6, 2008).

[9] http://www.lccr.com/OFAC%20complaints%203-18-08.pdf (last visited May 6, 2008).

process is cumbersome and painstaking, and no one is sure how exactly an individual is "cleared off the list." *Id*. OFAC tells individuals who are branded with the SDN label to contact each credit-reporting agency, because OFAC does not "clear" individuals. But then there is confusion and difficulty when the credit-reporting agencies, such as Experian, are contacted.

2. No-Fly and Selectee Lists

The Terrorist Screening Center coordinates the "no-fly" and "selectee" watch lists, which are most well-known for their use by airport security. These lists are also included in the NCIC, which is widely used by police. Thomas E. Bush III, Assistant Dir., Criminal Justice Info. Serv. Div., *Statement Before the S. Comm. on Homeland Sec. & Gov'tal Affairs*, 109th Cong. (June 29, 2005). Several government reports have reviewed the watch list process and the lists themselves and significant problems were found.

In September 2007, the Justice Department's Inspector General's review of the Terrorist Screening Center found that the government's watch lists of known or suspected terrorists remain filled with errors that the Inspector General said could obstruct the capture of terrorists. Office of Inspector General, Dep't of Justice, *Follow-Up Audit of the Terrorist Screening Center, Audit Report 07-41* (Redacted for Public Release) (Sept. 2007) [hereinafter "Justice Dept. Report on Watch Lists"]. "Furthermore, inaccurate, incomplete, and obsolete watchlist information increases the chances of innocent persons being stopped or detained during an encounter because of being misidentified as a watchlist identity." *Id*. at iii.

The Inspector General was highly critical of the system, detailing a number of errors in the watch lists and said the data collection and dissemination structure helped cause "inaccurate and incomplete watchlist records." *Id.* at ii-iii, 61. In fact, problems at the Center meant that "several known or suspected terrorists" were not on the lists, though they should be. *Id.* at ii. The Inspector General said, "The results of our testing of watchlist records, as well as the TSC finding that many records involved in its redress reviews required modification or removal, *indicate a deficiency in the integrity of watchlist information*" (emphasis added). *Id.* at xxii.

An April 2006 report by the Department of Homeland Security's Privacy Office on the impact of the watch lists explained that "individuals who are mistakenly put on watch lists or who are misidentified as being on these lists can potentially face consequences ranging from inconvenience and delay to loss of liberty." Privacy Office, Dep't of Homeland Sec., *Report Assessing the Impact of the Automatic Selectee and No Fly Lists on Privacy and Civil Liberties as Required Under Section 4012(b) of the Intelligence Reform and Terrorism Prevention Act of 2004* i (Apr. 27, 2006). The report described complaints "alleg[ing] misconduct or disrespect by airline, law enforcement, TSA or CBP officials" toward people mistakenly matched. *Id.* at 18.

Also, documents obtained by EPIC under the Freedom of Information Act show nearly a hundred complaints from airline passengers between November 2003 and May 2004 about the government's traveler screening security measures. Transp. Sec. Admin., Dep't of Homeland Sec., *Complaint Log: Nov. 2003 to May 2004,* obtained by

EPIC through FOIA litigation.[10] The complaints describe the bureaucratic maze passengers encounter if they happen to be mistaken for individuals on the list, as well as the difficulty they encounter trying to exonerate themselves through the redress process. One person named in the documents, Sister Glenn Anne McPhee, U.S. Conference of Catholic Bishops' secretary for education, spent nine months attempting to clear her name from a TSA watch list. The process was so difficult, Sister McPhee told a reporter, "Those nine months were the closest thing to hell I hope I will ever experience." Ryan Singel, *Nun Terrorized by Terror Watch*, Wired News, Sept. 26, 2005.

In a highly publicized case, a Canadian named Maher Arar brought the dangers of the error-filled watch lists to the world's attention. In September 2002, Arar was detained, interrogated and imprisoned for 12 days in the U.S, while en route home from a family holiday in Tunisia. Comm'n of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Factual Background, Vol. 1* 149 (2006).[11] The U.S. authorities used wholly erroneous data gathered by Canadian police and intelligence officials in its investigation of Arar.

After the 12 days of detention in the U.S., Arar was then handcuffed and shackled, put on a private jet, and flown to Syria where he was subjected to intense interrogation and locked in a tiny, grave-

---

[10] *Available at* http://www.epic.org/privacy/airtravel/foia/complaint_log.pdf (last visited May 6, 2008).

[11] *Available at* http://www.ararcommission.ca/eng/Vol_I_English.pdf (last visited May 6, 2008).

like cell for more than 10 months. Comm'n of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Factual Background, Vol. 2* 470-73 (2006).[12] In October 2003, he was finally released and sent back to Canada. *Id*. After extensive public pressure, the Canadian government agreed in January 2004 to an inquiry into the Arar case.

In 2006, the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar released a report detailing the erroneous evidence and the effect of disseminating this data through an information sharing structure among the Royal Canadian Mounted Police ("RCMP"), Canadian Security Intelligence Services ("CSIS") U.S. Federal Bureau of Investigation ("FBI"). Comm'n of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (2006). "The RCMP provided American authorities with information about Mr. Arar that was inaccurate, portrayed him in an unfairly negative fashion and over-stated his importance in the RCMP investigation," the Commission said. *Id*. at 13. While Arar was detained in New York, "the RCMP provided the U.S. Federal Bureau of Investigation (FBI) with information about him, some of which portrayed him in an inaccurate and unfair way." *Id*. at 14. Also, data sent from Canadian officials "indicated that Mr. Arar had been in the vicinity of

---

[12] *Available at* http://www.ararcommission.ca/eng/Vol_II_English.pdf (last visited May 6, 2008).

Washington, D.C. on September 11, 2001, which was false." *Id*. at 28.

Also, the U.S. was told that "Arar had declined to be interviewed in January 2002 and, soon after, had suddenly left Canada for Tunisia." This information was false. *Id*. at 28. In the end, the Commission of Inquiry Judge Dennis O'Connor, who led the investigation, concluded, "I am able to say categorically that there is no evidence to indicate that Mr. Arar has committed any offence or that his activities constitute a threat to the security of Canada." *Id*. at 59. Even after a request from the Canadian government to remove him from the list, the U.S. has kept Arar on its watch list. Even though Arar had been cleared by Canada and even though the U.S. did not have enough evidence to charge Arar with a crime, "We remain of the view that the continued watch listing of Mr. Arar is appropriate," wrote then-Attorney General Alberto Gonzales and DHS Secretary Michael Chertoff in a letter to the Canadian prime minister. Letter from Alberto Gonzales, U.S. Atty. Gen., and Michael Chertoff, Sec'y, Dep't of Homeland Sec., to Stockwell Day, Canadian Minister of Public Safety (Jan. 16, 2007). Arar remains on the U.S. watch list.

In 2005, Congress ordered the Government Accountability Office ("GAO") to investigate TSA's airline passenger screening programs. GAO found significant problems with handling of personal information and violations of privacy laws. Gov't Accountability Office, *Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information during Secure Flight Program Testing in Initial Privacy Notices, but Has Recently Taken Steps to More Fully Inform the Public*, GAO-05-864R (July 22,

2005). In September, GAO reviewed the watch list system and found "about half of the tens of thousands of potential matches sent to the center between December 2003 and January 2006 for further research turned out to be misidentifications." Gov't Accountability Office, *Terrorist Watch List Screening: Efforts to Help Reduce Adverse Effects on the Public,* GAO-06-1031 (Sept. 2006). According to the GAO, these misidentifications are a significant problem, and they:

> highlight the importance of having a process -- often referred to as redress -- for affected persons to express their concerns, seek correction of any inaccurate data, and request other actions to reduce or eliminate future inconveniences. Similarly, such a process would apply to other persons affected by the maintenance of watch list data, including persons whose names are actually on the watch list but should not be ("mistakenly listed persons") as well as persons who are properly listed.

Id. at 2.

Even federal air marshals are stymied by these watch lists. A recent news report described how air marshals have been kept off flights that they were assigned to protect because the air marshals' names were mistakenly matched to watch lists. Audrey Hudson, *Air marshals' names tagged on 'no-fly' list*, Wash. Times, Apr. 29, 2008. In January 2007, at a hearing of the Senate Commerce Committee, Sen. Ted Stevens complained that his wife, Catherine, is frequently mismatched to the watch list name "Cat Stevens." Beverley Lumpkin,

Aviation Security Chief Says No-Fly List is Being Reduced by Half, Associated Press, Jan. 18, 2007.

Senators Ted Kennedy and Representative Don Young are among those who have been improperly flagged by watch lists. Sen. Kennedy was able to resolve the situation only by enlisting the help of then-Homeland Security Secretary Tom Ridge. *See, e.g.,* Sara Kehaulani Goo, *Committee Chairman Runs Into Watch-List Problem*, Wash. Post, Sept. 30, 2004; Leslie Miller, *House Transportation Panel Chairman Latest to be Stuck on No-Fly List*, Associated Press, Sept. 29, 2004; Shaun Waterman, *Senator Gets a Taste of No-Fly List Problems*, United Press Int'l, Aug. 20, 2004.

III. Federal Government Is Increasingly Exempting Databases From Accuracy and Privacy Requirements

Even though the federal Privacy Act makes clear the need to ensure accurate records and the federal government recognizes that these databases are filled with errors, that has not stopped federal agencies from increasingly attempting to exempt themselves from Privacy Act of 1974, 5 U.S.C. 552a, provisions that require record accuracy. The agencies attempt to exempt themselves under §552a(j) (general exemptions) and §552a(k) (specific exemptions). Privacy Act of 1974. 5 U.S.C. §§ 552a(j), (k). Such exemptions from the general accuracy requirements applicable to government record-keeping systems undermine the argument that there are alternatives to the exclusionary rule that will produce the appropriate level of accuracy. Two prominent examples of such exempt systems are the NCIC database and the Automated Targeting System.

A. Federal Privacy Act Accuracy Obligations

The need to ensure the accuracy of personal information maintained by law enforcement agencies has long been a central concern in the development of privacy protection in the United States. *See, e.g.*, *The Computer and the Invasion of Privacy: Hearings Before a Subcom. of the H. Comm on Gov't Operations*, 89th Cong. (1966) (discussing, among various topics, "Information Sharing: The Hidden Challenge in Criminal Justice"); ARTHUR MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 36 (1971) ("The problem of contextual accuracy is certain to become more severe in the future as increasing numbers of remote terminals are linked to computer systems and local and regional data centers are amalgamated into national or international networks.").

The seminal 1973 report on privacy and government record-keeping, *Records, Computers, and the Rights of Citizens,* found that:

> In practice, however, the NCIC, like the National Driver Register, does not have effective control over the accuracy of all the information in its files. The NCIC is essentially an automated receiver, searcher, and distributor of data furnished by others. If a subscribing system enters a partially inaccurate record, or fails to submit additions to the NCIC files (e.g. the recovery of a stolen vehicle or the disposition of an arrest), there is not much the NCIC can do about it.

Dep't of Health, Educ. & Welfare, Secretary's Advisory Comm. on Automated Personal Data

Systems, *Records, Computers, and the Rights of Citizens* 17-18 (MIT 1973).

The report went on to say that: "Furthermore, the risk of propagating information that may lead to unjust treatment of an individual by law enforcement authorities in subscribing jurisdictions cannot be fully prevented." *Id.*

The report concluded that:

> Systems like the NCIC and the National Data Registry illustrate one of the potentially most significant effects of computerization of personal-data record keeping—the enhanced ability to gather, package and deliver information from one organization to another in circumstances where lines of authority and responsibility are overlapping or ambiguous, and where the significance attached to data disseminated by the system may vary among subscribing organizations. *Unless all organizations in a multi-jurisdictional system can be counted on to interpret and use data in the same way, the likelihood of unfair or inappropriate decisions about the individual to whom any given record pertains will be a problem*, and a particularly acute problem whenever records are incomplete or compressed.

Id. at 18-19 (emphasis added).

When it enacted the Privacy Act in 1974, Congress sought to address this problem and to impose clear obligations on Federal agencies that collect personal data and required agencies to be transparent in their information practices. S. Rep. No. 93-1183 at 1 (1974). In 2004, this Court underscored the importance of the Privacy Act's restrictions upon agency use of personal data to protect privacy interests, noting that:

> "[I]n order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary . . . to regulate the collection, maintenance, use, and dissemination of information by such agencies." Privacy Act of 1974, §2(a)(5), 88 Stat. 1896. The Act gives agencies detailed instructions for managing their records and provides for various sorts of civil relief to individuals aggrieved by failures on the Government's part to comply with the requirements.

Doe v. Chao, 540 U.S. 614, 618 (2004).

The Privacy Act is intended "to promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems and data banks of the Federal Government[.]" S. Rep. No. 93-1183 at 1. It is also intended to guard the privacy interests of citizens and lawful permanent residents against government intrusion. Congress found that "the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies," and recognized that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States." 5 U.S.C. § 552a. It thus sought to "provide certain protections for an individual against an invasion of personal privacy" by establishing a set of procedural and substantive rights. *Id.*

Among the most important obligations contained within the Privacy Act is the requirement that each agency that maintains a system of records shall:

> Maintain all records which are used by the agency in making decisions about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination.

5 U.S.C. §552a(e)(5).

But the problem continued, even after passage of the Privacy Act. As early as 1977, the Privacy Protection Study Commission (created by the Privacy Act of 1974), detailed ongoing problems with criminal justice information systems. Privacy Protection Study Comm'n, *Personal Privacy in an Information Society* (July 1977). One problem "emerges from even the briefest consideration of how information enters criminal justice systems and how it is used," the Commission said. *Id*. at 534. The Commission noted that there can be "little control over the accuracy and reliability of information when it passes from one information agency to another." *Id*. This is significant because criminal history information is "often the most revealing and potentially the most damaging recorded information exchanged by law enforcement agencies." *Id*. In this context of information sharing, the Privacy Act's requirements of accuracy and reliability of information are especially important.

B. The National Crime Information Center Is Exempt From Key Requirements

As we explained above, the National Crime Information Center ("NCIC") is a system that makes criminal history information widely available to police officers and law enforcement

officials across the United States. The Attorney General has the authority to "acquire, collect, classify, and preserve identification, criminal identification, crime, and other records" and "exchange such records and information with, and for the official use of, authorized officials of the Federal Government, the States, cities, and penal and other institutions." 28 U.S.C. § 534 (2002).

Furthermore, information can be entered into the system by either federal or state authorities. *Id.* A non-exhaustive list of information that Congress envisioned the NCIC to contain includes "arrests, convictions, and arrest warrants for stalking or domestic violence or for violations of protection orders for the protection of parties from stalking or domestic violence; and protection orders for the protection of persons from stalking or domestic violence, provided such orders are subject to periodic verification." *Id.*

The NCIC is an important and widely used database that is full of record inaccuracies. Yet, in 2003, the Department of Justice chose to exempt the NCIC from numerous mandates established by the Privacy Act, 5 U.S.C. § 552a, most notably accuracy requirements. As a result of this exemption, the FBI need not comply with 5 U.S.C. § 552a(e)(5), which requires an agency to "maintain all records which are used by the agency in making any determination about an individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual[.]" 5 U.S.C. § 552a(e)(5). The NCIC is also exempt from 5 U.S.C. § 552a(e)(1), which requires that a system of records contain "only such information about an individual as is relevant and necessary to accomplish a purpose of the agency[.]" *Id*. at $552(e)(1).

C. The Automated Targeting System Is Exempt From Key Requirements

The Automated Targeting System creates secret, terrorist "risk assessments" of tens of millions of U.S. citizens and foreign visitors annually. Dep't of Homeland Sec., *Notice of Privacy Act System of Records: U.S. Customs and Border Protection, Automated Targeting System*, 72 Fed. Reg. 43,650 (Aug. 6, 2007). These "risk assessments" to determine whether individuals will be subject to invasive searches of their persons or belongings, and whether U.S. citizens will be permitted to enter or exit the country. *Id.* at 43,651. As the agency notice describing the system makes clear, the Automated Targeting System profiles may be integrated with other government databases and used for a wide variety of purposes.

In the System of Records Notice for the Automated Targeting System, the Department of Homeland Security sought exemptions from key Privacy Act requirements to ensure accurate and reliable data. *Id.* at 43,653. The agency sought these exemptions even though the Automated Targeting System uses data from erroneous government watch lists.

As explained above, the government watch lists have been deemed full of errors by several government agencies. In fact, the Justice Department's Inspector General said in 2007 that there was "indicate[d] a deficiency in the integrity of watchlist information." Justice Dept. Report on Watch Lists at xxii. Even with knowledge of these deficiencies, the Department of Homeland Security still sought to, and did in the end, exempt the Automated Targeting System from the accuracy requirements of the Privacy Act.

CONCLUSION

In her concurrence in *Arizona v. Evans*, Justice O'Connor wrote:

> In recent years, we have witnessed the advent of powerful, computer-based recordkeeping systems that facilitate arrests in ways that have never before been possible. The police, of course, are entitled to enjoy the substantial advantages this technology confers. They may not, however, rely on it blindly. With the benefits of more efficient law enforcement mechanisms comes the burden of corresponding constitutional responsibilities.

514 U.S. 17-18.

Maintaining accurate record systems is one of the central requirements of information management. Moreover, the technology of government databases has changed dramatically since 1995, when the Court upheld the use of evidence obtained from an erroneous arrest record that was the product of a clerical mistake. It is no longer the case of one sheriff's clerk calling a clerk in another county. Today, the police have within their electronic reach access to an extraordinary range of databases. Mixed and mingled together are government and commercial databases filled with errors. Modern policing is a coordinated enterprise and it is critical that a commitment to accuracy is maintained throughout the criminal justice system.

Not only does erroneous data affect the rights of citizens, it also undermines effective investigations by creating confusion and mistakes. In recognition of the extraordinary consequences that may flow

from law enforcement officials acting upon such errors, the Court should enforce the exclusionary remedy in this case.

The need to safeguard privacy during a period of rapid technological change is self-evident.

> [W]e sense a great threat to privacy in modern America; we all believe that privacy is too often sacrificed to other values; we all believe that the threat to privacy is steadily and rapidly mounting; we all believe that action must be taken on many fronts now to preserve privacy.

SAMUEL ALITO, THE BOUNDARIES OF PRIVACY IN AMERICA 1 (1972) ("Report of the Chairman") (on file with *amici*).

Amici respectfully request this Court to grant Petitioner's motion to reverse the decision of the lower court.

Respectfully submitted,

MARC ROTENBERG
MELISSA NGO
ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140

Dated: May 16, 2008